Deployment & Operations References

Julia H. Allen, Software Engineering Institute [vita[1]]

2006-10-31

Content area bibliography.

[ACC 02]	American Chemistry Council. *Implementation Guide for Responsible Care® Security Code of Management Practices[2]: Site Security and Verification*, 2002.
[ACC 06]	American Chemistry Council's Chemical Information Technology Council. "Guidance for Addressing Cyber Security in the Chemical Industry[3], Version 3.0." ACC *ChemITC*, May 2006.
[Alberts 03]	Alberts, Christopher; Dorofee, Audrey; Stevens, James; & Woody, Carol. "Introduction to the OCTAVE® Approach[4]." Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.
[Alberts 04]	Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015[5]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.
[Alberts 05]	Alberts, Christopher & Dorofee, Audrey. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments* (CMU/SEI-2005-TN-032[6]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.
[Allen 01]	Allen, Julia. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison Wesley, 2001.

1. daisy:215 (Allen, Julia H.)
2. http://www.rctoolkit.com/pdfs/SSG.pdf
3. http://www.chemicalcybersecurity.com/cybersecurity_tools/ProgramCyberSecurityGuidanceFINAL.pdf
4. http://www.cert.org/octave/approach_intro.pdf
5. http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html
6. http://www.sei.cmu.edu/publications/documents/05.reports/05tn032.html

[Allen 03] Allen, Julia; Gabbard, Derek' & May, Christopher. *Outsourcing Managed Security Services* (CMU/SEI-SIM-012[7]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[Allen 05] Allen, J. *Governing for Enterprise* Security (CMU/SEI-2005-TN-023[8]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.

[BSI 98] British Standards Institute and International Organization for Standardization. *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security*. BS ISO/IEC TR 13335-3:1998(E), First edition, June 15, 1998.

[BSI 06] British Standards Institute. *Information security management systems – Part 3: Guidelines for information security risk management*. BS 7799-3:2006. BSI, March 17, 2006.

[Campbell 05] Campbell, Philip. "A COBIT Primer[9]." Sandia Report SAND2005-3455. Sandia National Laboratories, June 2005.

[Caralli 05] Caralli, Richard. "Focus on Resiliency: A Process-Oriented Approach to Security[10]." 32nd Annual Computer Security Institute Conference & Exhibition. Software Engineering Institute, Carnegie Mellon University, 2005.

[Caralli 06] Caralli, Richard. "Sustaining Operational Resiliency: A Process Improvement Approach to Security Management." (CMU/SEI-2006-TN-009[11]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, April 2006.

[CERT 05] CERT. *Survivability and Information Assurance Curriculum*[12]. Software Engineering Institute, Carnegie Mellon University, 2005. Most of the material in this article description is taken from the curriculum overview[13].

7. http://www.cert.org/archive/pdf/omss.pdf
8. http://www.sei.cmu.edu/publications/documents/05.reports/05tn023.html
9. http://www.itgi.org/
10. http://www.cert.org/archive/pdf/resiliency0511.pdf
11. http://www.sei.cmu.edu/publications/documents/06.reports/06tn009.html
12. http://www.cert.org/sia
13. http://www.cert.org/sia/Curriculum_Overview.pdf

[Chew 06] Chew, Elizabeth; Clay, Alicia; Hash, Joan; Bartol, Nadya; & Brown, Anthony. *Guide for Developing Performance Metrics for Information Security* (NIST Special Publication 800-80[14], Initial Public Draft). Gaithersburg, MD: National Institute of Standards and Technology, May 2006.

[CGTF 04] Corporate Governance Task Force. "Information Security Governance[15]: A Call to Action." National Cyber Security Partnership, April 2004.

[CISWG 04] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams[16]." November 17, 2004; updated January 10, 2005.

[Conner 06] Conner, Bill. "On compliance[17]: Get a step-by-step plan for meeting PCI standards." *SC Magazine*, August 7, 2006.

[CSCSP 06] Chemical Sector Cyber Security Program. "Guidance for Addressing Cyber Security in the Chemical Industry[18], Version 3.0." American Chemistry Council, Chemical Information Technology Council, May 2006.

[FFIEC 06] Federal Financial Institutions Examination Council. *IT Examination Handbook[19]: Information Security*. July 2006.

[GAO 99] U.S. Government Accounting Office. *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33[20]). November 1999.

[Goertzel 06] Goertzel, Karen Mercedes; Winograd, Theodore; McKinley, Holly Lynne; & Holley, Patrick. *Security in the Software Lifecycle[21]: Making Software Development Processes – and Software Produced by Them – More Secure*, Draft version

14. http://csrc.nist.gov/publications/nistpubs/index.html
15. http://www.cyberpartnership.org/
16. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661
17. http://www.scmagazine.com/us/news/article/576121/on-compliance-step-by-step-plan-meeting-pci-standards/
18. http://www.chemicalcybersecurity.com/online_information/guidance_docs.cfm
19. http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf
20. http://www.gao.gov/special.pubs/ai00033.pdf
21. daisy:87 (Security in the Software Lifecycle)

1.2. U.S. Department of Homeland Security, August 2006.

[Guel 01] Guel, Michele D. "A Short Primer for Developing Security Policies[22]." *The SANS Policy Primer*. The SANS Institute, 2001.

[Hazlewood 06] Hazlewood, Victor. *Defense-In-Depth[23]: An Information Assurance Strategy for the Enterprise*. La Jolla, CA: San Diego Supercomputer Center Security Technologies, 2006.

[IIA 05] The Institute of Internal Auditors. *Global Technology Audit Guides[24]: Change and Patch Management Controls: Critical for Organizational Success*. July 2005.

[IsecT 06] IsecT Ltd. Other security standards[25] (2006).

[ISF 05] Information Security Forum. *The Standard of Good Practice for Information Security[26], Revision 4.1*. January 2005.

[ISO 97] International Organization for Standardization. *Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security.* ISO/IEC TR 13335-2:1997(E), December 15, 1997.

[ISO 00] International Organization for Standardization. *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards.* ISO/IEC TR 13335-4:2000(E), March 1, 2000.

[ISO 04] International Standards Organization. *Information Technology – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®).* ISO/IEC 21827:2002. Also available through The International Systems Security Engineering Association (ISSEA) at http://www.sse-cmm.org/index.html.

[ISO 05a] International Organization for Standardization. *Information technology – Security techniques – Code of practice for information security management*. ISO/IEC 17799:2005(E), Second edition, June 15, 2005.

22. http://www.sans.org/resources/policies/Policy_Primer.pdf
23. http://security.sdsc.edu/DefenseInDepthWhitePaper.pdf
24. http://www.theiia.org/index.cfm?doc_id=5167
25. http://www.iso27001security.com/html/others.html
26. http://www.isfsecuritystandard.com/index_ns.htm

[ISO 05b] International Organization for Standardization. *Information technology – Security techniques – Information security management systems – Requirements*. ISO/IEC 27001:2005(E), First edition, October 15, 2005.

[ISO 05c] International Organization for Standardization. *Information technology – Service management* (ISO/IEC 20000-1:2005(E)), First edition, December 15, 2005. *Part 2: Code of practice* (ISO/IEC 20000-2:2005(E)), December 15, 2005.

[ITGI 04] Information Technology Governance Institute. *COBIT Security Baseline: An Information Security Survival Kit*. http://www.itgi.org/ (2004).

[ITGI 05a] Information Technology Governance Institute. *COBIT 4.0 Control Objectives for Information and related Technology*. ITGI, 2005. http://www.itgi.org[29] and http://www.isaca.org[30].

[ITGI 05b] IT Governance Institute & Office of Government Commerce. "Aligning COBIT®, ITIL®, and ISO 17799 for Business Benefit[31]: A Management Briefing from ITGI and OGC." ITGI & OGC, 2005.

[ITIL 99] IT Infrastructure Library. *Security Management*[32]. Norwich, Norfolk, England: Office of Government Commerce, 1999.

[ITIL 00] IT Infrastructure Library. *Service Support*[33]. Norwich, Norfolk, England: Office of Government Commerce, 2000.

[ITIL 01] IT Infrastructure Library. *Service Delivery*[34]. Norwich, Norfolk, England: Office of Government Commerce, 2001.

[ITPI 04] Behr, Kevin; Kim, Gene; & Spafford, George. *Visible Ops Handbook: Starting ITIL in Four Practical Steps*. IT Process Institute, 2004. Introductory and ordering information is available at http://www.itpi.org[35].

[Kim 04] Kim, Gene & Allen, Julia. "High-Performing IT

29. http://www.itgi.org/
30. http://www.isaca.org/
31. http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=22493&TEMPLATE=/ContentManagement/ContentDisplay.cfm
32. http://www.ogc.gov.uk/guidance_itil_4899.asp
33. http://www.ogc.gov.uk/guidance_itil_4899.asp
34. http://www.ogc.gov.uk/guidance_itil_4899.asp
35. http://www.itpi.org/

Organizations[36]: What You Need to Change to Become One." *BetterManagement.com*, April 30, 2004.

[Kim 06] Kim, Gene, et al. *IT Controls Performance Study: Identification of foundational controls that have the greatest impact on IT operations, security, and audit performance measures*. IT Process Institute, 2006. Ordering information is available at http://www.itpi.org/home/performance_study.php.

[Jones 05] Jones, Jack. "An Introduction to Factor Analysis of Information Risk[38] (FAIR): A framework for understanding, analyzing, and measuring information risk." Jack A. Jones, 2005.

[Lindner 06] Lindner, Martin; Losi, Stephanie; & Allen, Julia. "Proactive Remedies for Rising Threats." CERT Podcast Series[39]: Security for Business Leaders. August 2006.

[May 06] May, Christopher J.; Hammerstein, Josh; Mattson, Jeff; & Rush, Kristopher. *Defense-in-Depth: Foundations for Secure and Resilient Enterprises* (CMU/SEI-2006-HB-003[40]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

[McGraw 06] McGraw, Gary. *Software Security: Building Security In*. Boston, MA: Addison-Wesley, 2006. For Article 2, refer to Chapter 2, "A Risk Management Framework." For Articles 3 and 4, refer to Chapter 9, "Software Security Meets Security Operations."

[NIAC 05] National Infrastructure Advisory Council. "Risk Management Approaches to Protection[41]; Final Report and Recommendations by the Council." NIAC, October 11, 2005.

[NIST 03] National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems* (FIPS PUB 199[42]). Federal Information Processing Standards Publication, NIST, December 2003.

[NIST 06] National Institute of Standards and Technology. *Minimum Security Requirements for Federal*

36. http://www.bettermanagement.com/Library/Library.aspx?a=13&LibraryID=9429

38. http://nujia.norwich.edu/current/2_1_art01NUJIA.pdf

39. http://www.cert.org/podcast/

40. http://www.sei.cmu.edu/publications/documents/06.reports/06hb003.html

41. http://www.dhs.gov/interweb/assetlibrary/NIAC_RMWG_-_2-13-06v9_FINAL.pdf

42. http://csrc.nist.gov/publications/fips/

Information and Information Systems (FIPS PUB 200[43]). Federal Information Processing Standards Publication, NIST, March 2006.

[NSA] National Security Agency. "Defense in Depth[44]: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments."

[NSA 06] National Security Agency. "The 60 Minute Network Security Guide[45] (First Steps Towards a Secure Network Environment), Version 2.1." National Security Agency, May 15, 2006.

[OGC 05] Office of Government Commerce. *Information Technology Infrastructure Library (ITIL)*®.[46] Office of Government Commerce. Refer to http://www.ogc.gov.uk/index.asp?id=2261 and http://www.itsmf.com[48], specifically, "ITIL Best Practice for Security Management."

[PCI 06] Payment Card Industry (PCI) Data Security Standard[49], Version 1.1, PCI Security Standards Council, September 2006.

[Ravenel 06] Ravenel, J. Patrick. "Effective Operational Security Metrics." *Information Systems Security 15*, 3 (July/August 2006).

[Rogers 02] Rogers, Lawrence R. & Allen, Julia. "Securing Information Assets - Security Knowledge in Practice[50]." *Crosstalk: The Journal of Defense Software Engineering*, November 2002.

[Rogers 04] Rogers, Lawrence R. "Principles of Survivability and Information Assurance[51]." Software Engineering Institute, Carnegie Mellon University, 2004.

[Ross 06] Ross, Ron; Katzke, Stu; Johnson, Arnold; Swanson, Marianne; Stoneburner, Gary; Rogers, George; & Lee, Annabelle. *Recommended Security Controls for Federal Information Systems* (NIST Special Publication 800-53[52], Revision 1).

43. http://csrc.nist.gov/publications/fips/
44. http://nsa2.www.conxion.com/support/guides/sd-1.pdf
45. http://www.nsa.gov/snac/support/I33-011R-2006.pdf
46. ITIL is a registered trademark of OGC.
48. http://www.itsmf.com/
49. https://www.pcisecuritystandards.org/tech/index.htm
50. http://www.stsc.hill.af.mil/crosstalk/2002/11/rogers.html
51. http://www.cert.org/archive/pdf/SIAPrinciples.pdf
52. http://csrc.nist.gov/publications/nistpubs/index.html

National Institute of Standards and Technology, July 2006.

[Scott 01] Scott, Donna. "Network and System Management[53]: Often the Weakest Link in Business Availability." Gartner, July 3, 2001.

[Stern 01] Stern, Andrea. "Reinvesting the IT Dollar[54]: From IT Firefighting to Quality Strategic Services." *EDUCAUSE Quarterly*, Number 3, 2001.

[Stevens 93] Stevens, W. Richard. *TCP/IP Illustrated, Volume 1: The Protocols*. Boston, MA: Addison-Wesley, 1993.

[Stoneburner 02] Stoneburner, Gary; Goguen, Alice; & Feringa, Alexis. *Risk Management Guide for Information Technology Systems* (NIST Special Publication 800-30[55]). National Institute of Standards and Technology, July 2002.

[Stoneburner 04] Stoneburner, Gary; Hayden, Clark; & Feringa, Alexis. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A* (NIST Special Publication 800-27[56], Revision A). National Institute of Standards and Technology, June 2004.

[Swanson 06] Swanson, Marianne; Hash, Joan; & Bowen, Pauline. *Guide for Developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18[57], Revision 1). National Institute of Standards and Technology, February 2006.

[Visa 06] Visa U.S.A. Inc. "Visa U.S.A Cardholder Information Security Program Payment Application Best Practices, Version 1.3[58]." May, 2006.

[Womack 91] Womack, James P.; Jones, Daniel T.; & Roos, Daniel. *The Machine That Changed the World: The Story of Lean Production*. New York, NY: Harper Perennial, 1991.

[Worthen 05] Worthen, Ben. "ITIL Power[59]." *CIO Magazine*, September 1, 2005.

53. http://www.gartner.com/DisplayDocument?id=334197&ref=g_search
54. http://www.educause.edu/ir/library/pdf/eqm0130.pdf
55. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
56. http://csrc.nist.gov/publications/nistpubs/index.html
57. http://csrc.nist.gov/publications/nistpubs/index.html
58. http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_Payment_Application_Best_Practices.pdf
59. http://www.cio.com/archive/090105/itil_frameworks.html

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	false
Content Areas	Best Practices/Deployment & Operations
SDLC Relevance	Deployment
Workflow State	Publishable
Sort Order	12

1. http://www.sei.cmu.edu/about/legal-permissions.html